Abstract

A system and method for declaring alert indications that occur in an enterprise comprising translating a number of device outputs into a common format event using a number of translation files, and generating a number of knowledge-containing common format events based on matches between the common format events and knowledge base tables. A set of rules determines whether the knowledge base common format events rise to an alert indication for further automated correlation and analysis.